Mail Stop: Appeal Brief-Patents

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	Jardin *et al.*	
Serial No.:	09/721,785	Group Art Unit: 2135
Filed:	November 22, 2000	Examiner: Akpati, Odaiche T.
Title:	**Link-Lock Device And Method Of Monitoring And Controlling A Link For Failures And Intrusions**	

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to the Notice of Appeal filed on March 12, 2005, Applicants (hereafter "Appellants") hereby submit this Appeal Brief in support of an Appeal from the Final Decision by the Examiner in the above-captioned patent application. Appellant respectfully requests consideration of this Appeal by the Board of Patent Appeals and Interferences for allowance of the claims in the above-captioned patent application.

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this Appeal. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefore are hereby authorized to be charged to Deposit Account No. 02-2666.

I. Real Party in Interest

The real party in interest is the assignee of the full interest in the invention, Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95054-1549.

II. Related Appeals and Interferences

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

III. Status of Claims

Claims 1-18 are pending in the application and were finally rejected in an Office Action mailed January 13, 2005. Claims 1-18 are the subject of this appeal. A copy of Claims 1-18 as they stand on appeal are set forth in the Claims Appendix (Appendix A).

IV. Status of Amendments

A first Office Action was mailed on April 22, 2004. In response to the first Office Action, no claim amendments were made. A final Office Action was mailed on January 13, 2005. In response to the final Office Action, no claim amendments were made. Thus, the attached Claims reflect the status of the claims as filed on November 22, 2000.

V. Summary of Claimed Subject Matter

The invention relates to a link-lock system coupled to a network device to monitor and control the security mode of a link between the network device and a server or client computer. As recited in independent claim 1, the link-lock system for a network includes a computer, such as a server or a client computer (FIG. 2, block 210; FIG. 3, block 210; Specification, page 4, lines 9-14, a network interface device (FIG. 2, block 204; FIG. 3, block 204; Specification, page 4, lines 2-5) to provide the computer with access to the network (FIG. 2, network infrastructure block 201; Specification, page 4, lines 2-5), a bus monitor (FIG. 3, block 300; Specification, page 5, lines 1-3) to monitor a first link (FIG. 2, link 208; FIG. 3, link 208; Specification, page 4, lines 10-14) between the network interface device (FIG. 2, block 204; FIG. 3, block 204; Specification, page 4, lines 2-5) and the computer (FIG. 3, block 210; Specification, page 5, lines 19-24). The bus monitor reports detected failures or intrusions (FIG. 3, block 300, Specification, page 5, lines 19-20). The link-lock system also includes a security switch (FIG. 3, block 302; Specification, page 5, lines 1-3) to switch the first link from a non-secured mode to a secured mode when a report of the detected failures or intrusions is received from the bus monitor (Specification, page 5, lines 12-24; FIG. 3, blocks 302, 300, and 208).

Independent claim 8 is a system claim for server (FIG. 3, Specification, page 4, line 24 – page 6, line 5. The system includes an interface device (FIG. 2, block 204; FIG. 3, block 204; Specification, page 4, lines 2-5) to provide the server with access to a network (FIG. 2, block 210; FIG. 3, block 210; Specification, page 4, lines 10-14) and a controller (FIG. 3, block 306; Specification page 5, lines 1-3) to monitor a link between the interface device and the server (FIG. 3, block 204, block 210, block 306;

Specification, page 5, line 20 – page 6, line 5. The controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link (FIG. 3, block 204, block 210, block 306, Specification, page 5, line 20 – page 6, line 5).

With respect to independent claim 12, the invention as claimed is a method. The method includes monitoring a link between a network device and a computer (FIG. 4, block 400; Specification, page 6, lines 6-9). The link is directed to use a secured protocol when failures or intrusions are detected on the link (FIG. 4, blocks 402 and 404; Specification, page 6, lines 9-11). The link is directed to revert back to a non-secured protocol when the detected failures or intrusions are corrected (FIG. 4, block 406; Specification, page 6, lines 11-14, Specification, page 3, lines 15-22).

With respect to independent claim 16, the invention as claimed is directed to an apparatus having a machine readable storage medium having executable instructions that enable the machine to monitor a link between a network device and a server (FIG. 4, block 400; Specification, page 6, lines 6-9). The link is directed to use a secured protocol when failures or intrusions are detected on the link (FIG. 4, blocks 402 and 404; Specification, page 6, lines 9-11). The link is directed to revert back to a non-secured protocol when the detected failures or intrusions are corrected (FIG. 4, block 406; Specification, page 6, lines 11-14; Specification, page 3, lines 15-22).

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 1-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,583,714 to Gabou *et al.* (hereinafter "Gabou") in view of U.S. Patent No. 6,079,020 to Liu.

VII. Argument

A. Claims 1-18 are patentable under 35 U.S.C. 103(a) over Gabou in view of Liu.

In the Final Office Action dated January 13, 2005, the Examiner stated, with regards to independent claims 1, 8, 12, and 16 that Gabou teaches all of the limitations in the claims except that Gabou does not teach the limitation of "a network interface device to provide the computer [or server] with access to the network." Final Office Action dated January 13, 2005, pages 3-4, 6, and 8. The Examiner maintained his rejection in the Advisory Action dated March 30, 2005.

Three criteria must be met to establish a *prima facie* case of obviousness. MPEP 2143. There must be some suggestion or motivation, either in the references themselves or in the knowledge available to one of skill in the art, to combine the references. *Id.* There must be a reasonable expectation of success. *Id.* And, lastly, the prior art references must teach or suggest all the claim limitations. *Id.* "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure." MPEP 2143 (*citing In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

The Examiner has failed to establish a *prima facie* case of obviousness for at least the following reasons: (1) the references of Gabou and Liu do not suggest the

combination or motivate one skilled in the art to combine them and (2) Gabou and Liu combined do not teach or suggest all of the claim limitations of independent claims 1, 8, 12, and 16.

1. The References of Gabou and Liu Do Not Suggest the Combination or Motivate One Skilled in the Art to Combine Them

As indicated above, the teachings or suggestions to combine must be found in Gabou and Liu, not in Appellants' patent application. Gabou teaches a method for protecting a radiocommunications terminal against unauthorized use. *Gabou*, Abstract, col. 1, lines 47-49. When no user information is being transmitted, the radiocommunications terminal is automatically switched to a secure mode in which sending call data is prohibited and incoming calls or signaling data are authorized. *Id.* at col. 1, lines 52-57, lines 60-67. The secure mode is cancelled by entering a predetermined code. *Id.* at col. 1, lines 57-58. Thus, in a secure mode the radiocommunications terminal can receive calls, but it cannot be used to make a call by a user who does not know the predetermined code. *Id.* at col. 1, lines 60-67. In one embodiment, an exception is made for emergency calls. *Gabou*, col. 2, lines 7-9. During a secure mode a user may make an emergency call to an emergency service. *Id.*

Liu discloses a method and apparatus for managing a virtual private network operating over a public data network augmented to include a plurality of virtual private network gateways. *Liu*, Abstract; col. 3, lines 1-8. The virtual private network gateways enable communications across the virtual private network to be channeled through the gateways. *Id.* at col. 3, lines 8-10.

Appellants submit that the Examiner has combined Gabou and Liu based on the Appellants' application disclosure. The Examiner's primary reference is Gabou. The Examiner admits that Gabou does not teach "a network interface device to provide the computer with access to the network" in the Final Office Action dated January 13, 2005. The Examiner then states that Liu teaches this feature. Appellants assert that Gabou teaches the protection of a radiocommunications terminal from unauthorized use, and defines a radiocommunications terminal to mean "Personal Handy-Phone System (PHS) cordless telephones, Digital European Cordless Telecommunications (DECT) cordless telephones, Global System for Mobile Communications (GSM) cellular mobile telephones, Cordless Telephony System (CTS) cellular mobile telephones, and pagers. *Gabou*, col. 1, lines 10-16. The radiocommunications terminal disclosed in Gabou uses incoming calls and messages and outgoing calls and messages as a means of communicating over the telephone network. *Gabou*, col. 1, lines 60-67; col. 3, line 34 – col. 4, line 36. Liu, on the other hand, teaches a method and apparatus for managing virtual private networks (VPNs) operating over a public data network augmented to include a plurality of virtual private network gateways. *Liu*, Abstract; col. 3, lines 1-8. VPNs are employed in computer networks and are built on top of public networks, such as the Internet, to protect data transmitted over the public networks. *Liu*, col. 2, lines 16-19. Liu discloses a VPN (Virtual Private Network) management station that uses a network interface card to couple the VPN management station to a network. *Liu*, col. 8, lines 47-58. Since Gabou does not disclose a network interface device, a computer, a virtual private network or a virtual private network gateway and Liu does not disclose a radiotelecommunications terminal, Appellants assert that the Examiner has combined

Gabou and Liu based on Appellants' application disclosure. There is no teaching in Gabou that would suggest combining it with the teachings of Liu other than the fact that Appellants' invention uses a network interface device, Gabou does not, but Liu does.

For the reasons stated above, Appellants strongly assert that there is no motivation to modify Gabou with the teachings of Liu. Therefore, the Examiner has failed to establish a *prima facie* case of obviousness. Thus, claims 1-18 are patentable over the cited combination of references (*i.e.,* Gabou and Liu).

2. Gabou and Liu Combined Do Not Teach or Suggest All of the Claim Limitations of Independent Claims 1, 8, 12, and 16

Claim 1

With regards to independent claim 1, the Examiner states on pages 3-4 of the Final Office Action that Gabou teaches Appellants' elements of "a computer", "a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions", and "a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor. Appellants respectfully disagree.

Gabou teaches a method for protecting a radiocommunications terminal against unauthorized use, the radiocommunications terminal being cordless phones, cellular mobile phones, and pagers. *Gabou*, Abstract; col. 1, lines 10-16 and 46-51. According to Gabou, the terminal is automatically switched to a secure mode when no user information is being transmitted or when end-of-call information is detected. *Gabou*, col.

1, lines 52-57; col. 3, lines 49-56. Gabou also teaches that the secure mode is cancelled by the user when the user enters a predetermined code. *Gabou*, col. 1, lines 56-57; col. 3, lines 45-46.

Appellants respectfully assert that Gabou does not teach or suggest at least the following elements of Appellants' claimed invention:

> a computer;
> a network interface device to provide the computer with access to the network;
> a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions; and
> a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

Unlike the present invention, which refers to computers in a client/server model, Gabou teaches radiocommunications terminals comprising cordless phones, cellular mobile phones, and pagers. *Gabou*, col. 1, lines 10-16. Although a computer may include, or even emulate, a radiocommunications terminal, a radiocommunications terminal, or telephone/pager as defined by Gabou, is not a computer.

Gabou also does not teach or suggest "a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions." Contrary to the present invention, Gabou is not monitoring for failures or intrusions. Instead, Gabou is monitoring to determine whether user information is being transmitted from a terminal, and if it is not, then Gabou teaches switching to a secure mode. *Gabou*, col. 1, lines 52-57. Gabou also teaches that when end-of-call information is detected, the radiocommunications terminal is switched to a secure mode. *Gabou*, col. 3, lines 49-56. Unlike the present invention, Gabou prevents

intrusions from ever happening by switching to a secure mode when no user information is being transmitted or when an end-of-call is detected. Thus, Gabou does not monitor for an intrusion as recited in Appellants' claim 1. Instead Gabou prevents an intrusion from occurring by switching to a secure mode when no user information is being transmitted or when an end-of-call is detected. Thus, instead of monitoring for failures or intrusions, Gabou is monitoring for whether user information is being transmitted or for end-of-call information.

Gabou also does not teach or suggest "a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor." As indicated above, unlike the present invention, Gabou does not teach or suggest *detecting failures or intrusions*, and therefore, cannot teach or suggest switching the first link from a non-secured mode to a secured mode *when a report of said detected failures or intrusions is received from the bus monitor*. Instead, Gabou teaches switching to a secure mode when no user information is being transmitted or when an end-of-call is detected.

The Examiner further states, on page 4 of the Final Office Action, that Gabou does not teach Appellants' element of: "a network interface device to provide the computer with access to the network." Appellants respectfully agree that Gabou does not teach this element, as indicated above. The Examiner indicates that this element is taught by Liu.

Appellants respectfully disagree. Liu does not solve the deficiencies of Gabou. Liu teaches a method and apparatus for managing virtual private networks operating over

public data networks. *Liu*, Abstract, col. 3, lines 2-5. Liu does not teach or suggest Appellants' elements of:

> a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions; and
>
> a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

Thus, neither Gabou nor Liu, separately or in combination, teach or suggest Appellants' claimed invention as recited in independent claim 1. For at least the foregoing reasons, Appellants respectfully submit that independent claim 1, and the claims that depend therefrom (claims 2-7) are patentable over Gabou and Liu.

Independent Claim 8

With respect to independent claim 8, the Examiner, on page 6 of the Final Office Action, states that Gabou teaches Appellants' element of "a controller to monitor a link between the interface device and the server, where said controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link. Appellants respectfully disagree.

Unlike the present invention, Gabou does not teach a server. Instead, Gabou teaches radiocommunications terminals comprising cordless phones, cellular mobile phones, and pagers. *Gabou*, col. 1, lines 10-16. Also, Gabou does not teach "a controller to monitor a link ... , where said controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link." As indicated above, contrary to the present invention, Gabou is not monitoring for failures or

intrusions. Instead, Gabou is monitoring to determine whether user information is being transmitted from a terminal or whether end-of-call information is detected. If no user information is being transmitted from the terminal or if an end-of-call is detected, then Gabou teaches switching to a secure mode. *Gabou*, col. 1, lines 52-57; col. 3, lines 49-56. Unlike the present invention, Gabou prevents intrusions from ever happening by switching to a secure mode when no user information is being transmitted or when an end-of-call is detected. Thus, Gabou does not monitor for failures or intrusions, and therefore, does not switch "from a non-secured protocol to a secured protocol when failures or intrusions are detected" as recited in Appellants' claim 8. Instead Gabou is proactive in that it prevents an intrusion from occurring by switching to a secure mode when no user information is being transmitted or when an end-of-call is detected. The present invention is reactive in that it "switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link." Also, unlike the present invention which switches from a non-secured protocol (*e.g.*, HTTP) to a secured protocol (HTTP-S), Gabou teaches switching to a secure mode that prohibits sending at least one type of user information and authorizes sending at least one type of terminal information. *Gabou*, col. 1, lines 52-59.

The Examiner further states, on page 6 of the Final Office Action, that Gabou does not teach Appellants' element of: "an interface device to provide the server with access to a network." Appellants respectfully agree that Gabou does not teach this element, as indicated above. The Examiner indicates that this element is taught by Liu.

Appellants respectfully disagree. Liu does not solve the deficiencies of Gabou. Liu teaches a method and apparatus for managing virtual private networks operating over

public data networks. *Liu*, Abstract, col. 3, lines 2-5. Liu does not teach or suggest Appellants' elements of "a controller to monitor a link between the interface device and the server, where said controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link."

Thus, neither Gabou nor Liu, separately or in combination, teach or suggest Appellants' claimed invention as recited in independent claim 8. For at least the foregoing reasons, Appellants respectfully submit that independent claim 8, and the claims that depend therefrom (claims 9-11) are patentable over Gabou and Liu.

Independent Claims 12 and 16

With respect to independent claim 12, the Examiner, on page 8 of the Final Office Action, states that Gabou teaches Appellants' elements of: "first directing the link to use a secured protocol when failures or intrusions are detected on the link" and "second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected." Appellants respectfully disagree.

As indicated above, contrary to the present invention, Gabou is not detecting failures or intrusions. Instead, Gabou is detecting whether user information is being transmitted from a terminal or an end-of-call. If no user information is being transmitted from the terminal or if an end-of-call is detected, then Gabou teaches switching to a secure mode. *Gabou*, col. 1, lines 52-57; col. 3, lines 49-56. Unlike the present invention, Gabou prevents intrusions from ever happening by switching to a secure mode when no user information is being transmitted or when an end-of-call is detected. Thus, Gabou does not detect failures or intrusions, and therefore, does not provide for "first

directing the link to use a secured protocol *when failures or intrusions are detected on the link*" or "second directing the link to revert to a non-secured protocol *when said detected failures or intrusions have been corrected.*" Furthermore, unlike the present invention, Gabou teaches canceling the secure mode by entering a predetermined code (*Gabou*, col. 1, lines 56-57), and not when detected failures or intrusions have been corrected (as recited in claim 12).

The Examiner further states, on page 8 of the Final Office Action, that Gabou does not meet the limitations of a network device. Appellants respectfully agree that Gabou does not teach this element, as indicated above. The Examiner indicates that this element is taught by Liu.

Appellants respectfully disagree. Liu does not solve the deficiencies of Gabou. Liu teaches a method and apparatus for managing virtual private networks operating over public data networks. *Liu*, Abstract, col. 3, lines 2-5. Liu does not teach or suggest Appellants' elements of "monitoring a link between a network device and a computer," "first directing the link to use a secured protocol when failures or intrusions are detected on the link," or "second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected."

Thus, neither Gabou nor Liu, separately or in combination, teach or suggest Appellants' claimed invention as recited in independent claim 12. Appellants' independent claim 16 recites elements similar to the elements of claim 12. Thus, for at least the foregoing reasons, Appellants respectfully submit that independent claims 12 and 16, and the claims that depend therefrom (claims 13-15 and claims 17-18, respectively), are patentable over Gabou and Liu.

Conclusion

In view of the foregoing, favorable reconsideration and reversal of the rejections is respectfully requested. Early notification of the same is earnestly solicited. If there are any questions regarding the present application, the Examiner and/or the Board is invited to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

Intel Corporation

/Crystal D. Sayles, Reg. No. 44,318/
Crystal D. Sayles
Senior Attorney
Intel Americas, Inc.
(202) 986-3179

Dated: September 12, 2005

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on:

September 12, 2005
Date of Deposit

Catherine Jennings
Name of Person Mailing Correspondence

Catherine Jennings 9-12-05
Signature Date

Appendix A: Claims Appendix

1. A link lock system for a network, comprising:

a computer;

a network interface device to provide the computer with access to the network;

a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions; and

a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

2. The system of claim 1, wherein said computer is a server.

3. The system of claim 1, wherein the network operates in a secured mode using an HTTP-S protocol.

4. The system of claim 1, wherein said non-secured mode of the first link between the network device and the computer uses HTTP protocol.

5. The system of claim 4, wherein said secured mode of the first link between the network device and the computer uses HTTP-S protocol.

6. The system of claim 1, further comprising:

a controller that receives the report from the bus monitor and sends control signals to the network interface device, the security switch, and the computer.

7. The system of claim 6, further comprising:

an encryption element in the computer, where said encryption element converts data placed on said first link to a secured protocol when the control signal is received from said controller.

8. A system for a server, comprising:

an interface device to provide the server with access to a network; and

a controller to monitor a link between the interface device and the server, where said controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link.

9. The system of claim 8, wherein the network is Internet, such that the non-secured protocol includes HTTP and the secured protocol includes HTTP-S.

10. The system of claim 8, wherein said controller sends a control signal to the server when failures or intrusions are detected on the link.

11. The system of claim 10, further comprising:

an encryption element in the server, where said encryption element converts data placed on said link by the server to a secured protocol when the control signal is received from said controller.

12. A method, comprising:

monitoring a link between a network device and a computer;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

13. The method of claim 12, wherein said non-secured protocol includes HTTP protocol.

14. The method of claim 12, wherein said secured protocol includes HTTP-S protocol.

15. The method of claim 12, wherein the computer is a server.

16. An apparatus comprising a machine-readable storage medium having executable instructions that enable the machine to:

monitor a link between a network device and a server;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

17. The apparatus of claim 16, wherein said non-secured protocol includes HTTP protocol.

18. The apparatus of claim 16, wherein said secured protocol includes HTTP-S protocol.

Appendix B: Evidence Appendix

No evidence has been submitted in the present appeal.

Appendix C: Related Proceedings Appendix

There are no related proceedings.